THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

In re Great Expressions Data Security Incident Litigation	Case No.: 2:23-cv-11185 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Vanessa Brito, Crystal Coffey, Jacqueline Williams, and Aprill Denson, as next friend of C.D., a minor, ("Plaintiffs") bring this Class Action Complaint against ADG, LLC d/b/a Great Expressions Dental Centers ("ADG") and Great Expressions Dental Centers, P.C. ("GEDC") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] of current and former employees and patients of Defendants' customers/licensees (the "Dental Centers"), including (1) for employees: names, Social Security numbers, driver's

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

license numbers, passport numbers, and/or bank account and routing number and (2) for patients: patient names, dates of birth, contact information, mailing addresses, Social Security numbers, driver's license numbers, financial account information, credit or debit card numbers, diagnosis and treatment information, medical and dental history, dental examination information, charting information, treatment plans, x-ray images, dates of service, provider names, GEDC office of treatment, billing records, costs of services, prescription information and/or health insurance information.

2. According to Defendants' website, Great Expressions Dental Centers provides dental care at more than 300 locations in Connecticut, Florida, Georgia, Michigan, Massachusetts, New York, New Jersey, Ohio, and Texas.

3. According to Defendants' website, ADG "provides administrative and business support services and licenses the Great Expressions Dental Centers® brand name to independently owned and operated dental practices."[2]

4. Prior to and through February 22, 2023, Defendants obtained the PII of Plaintiffs and Class Members, including by collecting it directly from the Dental Centers and/or Plaintiffs and Class Members.

5. Prior to and through February 22, 2023, Defendants stored the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment

[2] *See* https://www.greatexpressions.com/about-us/ (last visited May 18, 2023).

on Defendants' network.

6. On or before February 22, 2023, Defendants learned of a data breach on their network that occurred between February 17, 2023 and February 22, 2023 (the "Data Breach").

7. Defendants determined that, during the Data Breach, an unknown actor acquired the PII of Plaintiffs and Class Members.

8. On or around May 12, 2023, Defendants began notifying Plaintiffs and Class Members of the Data Breach.

9. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII that may have been accessed and/or acquired by an unauthorized actor included (1) for employees: names, Social Security numbers, driver's license numbers, passport numbers, and/or bank account and routing number and (2) for patients: patient names, dates of birth, contact information, mailing addresses, Social Security numbers, driver's license numbers, financial account information, credit or debit card numbers, diagnosis and treatment information, medical and dental history, dental examination information, charting information, treatment plans, x-ray images, dates of service, provider names, GEDC office of treatment, billing records, costs of services, prescription

information and/or health insurance information.

10. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the likely loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

11. The PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

12. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

13. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware

containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

14. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

15. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal

use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

16. Plaintiff Brito is a citizen of Florida residing in Tampa, Florida.

17. Plaintiff Coffey is a citizen of Michigan residing in Taylor, Michigan.

18. Plaintiff Williams is a citizen of Texas residing in Texas.

19. Plaintiff Denson is a citizen of Florida residing in Florida.

20. Defendant ADG is a Michigan limited liability company with a principal place of business in Southfield, Michigan.

21. Defendant GEDC is a Michigan professional corporation with a principal place of business in Southfield, Michigan.

22. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

23. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendants to establish minimal diversity.

25. Under 28 U.S.C. § 1332(d)(10), Defendant ADG is a citizen of Michigan because it is a limited liability company formed under Michigan law with its principal place of business in Southfield, Michigan.

26. Under 28 U.S.C. § 1332(d)(10), Defendant GEDC is a citizen of Michigan because it is a professional corporation formed under Michigan law with its principal place of business in Southfield, Michigan.

27. The Eastern District of Michigan has personal jurisdiction over Defendants because they conducts substantial business in Michigan and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

28. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants operate in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendants collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

29. Defendants collected the PII of Plaintiffs and Class Members, including the Dental Centers' current and former employees and patients and others.

30. Plaintiffs and Class Members relied on this sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

31. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

32. On or about May 12, 2023, Defendants sent Plaintiffs and Class Members a notice of the Data Breach (the "Notice of Data Breach"). Defendants informed Plaintiffs and other employee Class Members that:

> We are writing to notify you about an incident that may have involved some of the information we maintain in Human Resources ("HR") related to our current and former Team Members. This notice explains the incident,

> our response, and the additional steps you can take to protect your information.
>
> On April 19, 2023, we completed our analysis or certain HR filed that may have been involved in a security incident that disrupted the operations of some of our TI systems and determined that your information may have been contained in those files. We initially identified the incident when we experienced unusual activity on our systems. We immediately took steps to secure our systems, launched an investigation with the assistance of a third-party forensic investigator, and notified law enforcement. The investigation determined that an unauthorized party accessed some of our systems between February 17, 2023 and February 22, 2023, and may have accessed or removed some files. Our analysis of those files determined that may have contained your information maintained by HR, including some or all of the following: your name, Social Security number, driver's license number, and/or passport number. If you elected to use direct deposit, your bank account number and routing number may have also been involved in the incident.

33. Similarly, Defendants informed patient Class Members that:

> On May 12, 2023, we began mailing notification letters to patients whose information may have been involved in a security incident that disrupted the operations of some of our IT systems.
>
> We initially identified the incident when we experienced unusual activity on our systems, and we immediately took steps to secure our systems, launched an investigation with the assistance of a third-party forensic investigator, and notified law enforcement. The investigation determined that an unauthorized party accessed some of our systems between February 17, 2023 and February 22, 2023, and may have accessed or removed some files. We then initiated a review and analysis of those files to determine what information they contained, which is still in progress.

> On April 19, 2023, through our ongoing analysis of the files that may have been involved in the incident, we determined that the files contained information belonging to some GEDC patients. The information varied per patient, but could have included one or more of the following: patient names, dates of birth, contact information, mailing addresses, Social Security numbers, driver's license numbers, financial account information, credit or debit card numbers, diagnosis and treatment information, medical and dental history, dental examination information, charting information, treatment plans, x-ray images, dates of service, provider names, GEDC office of treatment, billing records, costs of services, prescription information and/or health insurance information.

34. Defendants admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members.

35. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

36. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

37. Defendants did not use reasonable security procedures and practices

appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

38. Because Defendants had a duty to protect Plaintiff's and Class Members' PII, Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

39. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

40. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[3]

41. In April 2020, ZDNet reported, in an article titled "Ransomware

[3] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[4]

42. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[5]

43. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

---

[4] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[5] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

44. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendants' type of business had cause to be particularly on guard against such an attack.

45. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

46. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendants Acquire, Collect, and Store the PII of Plaintiffs and Class Members.

47. Defendants acquired, collected, and stored the PII of Plaintiffs and Class Members.

48. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

49. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential

and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

51. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans

[6] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

52. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have

[7] *Id.* at 3-4.

implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce

malicious network traffic….[8]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts

[8] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[9]

54. Given that Defendants were storing the PII of current and former employees and patients and others, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

55. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of current and former employees and patients and others, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

56. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-

[9] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

accessible environment when there was a reasonable need to do so.

57. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

60. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage

[10] 17 C.F.R. § 248.201 (2013).

[11] *Id.*

to victims may continue for years.

Value of Personal Identifiable Information

61. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

63. This data demands a much higher price on the black market. Martin

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[15]

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years.

66. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

[15] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

67. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

68. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

69. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained on Defendants' network, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

70. To date, Defendants have offered Plaintiffs and Class Members only one year of identity monitoring through Kroll. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

71. The injuries to Plaintiffs and Class Members were directly and

proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Plaintiff Brito's Experience

72. Plaintiff Brito last worked for and was a patient at one of the Dental Centers in approximately 2012 or 2013 and received Defendants' Notice of Data Breach, dated May 11, 2023, on or about that date. The notice stated that Plaintiff Brito's personal information was impacted by the Data Breach, including name, Social Security number, driver's license number, and/or passport number.

73. As a result of the Data Breach, Plaintiff Brito's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Brito's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Brito will have to worry about when and how her sensitive information may be shared or used to her detriment.

74. As a result of the Data Breach notice, Plaintiff Brito spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

75. Additionally, Plaintiff Brito is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

76. Plaintiff Brito stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

77. Plaintiff Brito suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

78. Plaintiff Brito has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

79. Plaintiff Brito has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Coffey's Experience

80. Plaintiff Coffey was a patient of and last worked for one of the Dental Centers in 2019 and received Defendants' Notice of Data Breach, dated May 11, 2023, on or about that date. The notice stated that Plaintiff Coffey's personal information was impacted by the Data Breach, including name, Social Security number, driver's license number, and/or passport number.

81. As a result of the Data Breach, Plaintiff Coffey's sensitive information

may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Coffey's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Coffey will have to worry about when and how her sensitive information may be shared or used to her detriment.

82. As a result of the Data Breach notice, Plaintiff Coffey spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

83. Additionally, Plaintiff Coffey is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

84. Plaintiff Coffey stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

85. Plaintiff Coffey has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

86. Plaintiff Coffey has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is

protected and safeguarded from future breaches.

Plaintiff Williams' Experience

87. Plaintiff Williams is an employee of Defendant and received Defendants' Notice of Data Breach, in May of 2023. The notice stated that Plaintiff Williams' personal information was impacted by the Data Breach, including name, Social Security number, driver's license number, and/or passport number.

88. As a result of the Data Breach, Plaintiff Williams' sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Williams' sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Williams will have to worry about when and how her sensitive information may be shared or used to her detriment.

89. As a result of the Data Breach notice, Plaintiff Williams spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

90. Additionally, Plaintiff Williams is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

91. Plaintiff Williams stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently

chooses unique usernames and passwords for her various online accounts.

92. Plaintiff Williams has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

93. Plaintiff Williams has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Denson's Experience

94. Plaintiff Denson was a customer of Defendant and received Defendants' Notice of Data Breach, in May of 2023. The notice stated that Plaintiff Denson personal information was impacted by the Data Breach, including name, Social Security number, driver's license number, and/or passport number.

95. As a result of the Data Breach, Plaintiff Denson's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Denson's sensitive information has been irreparably harmed. For the rest of their life, Plaintiff Denson will have to worry about when and how her sensitive information may be shared or used to their detriment.

96. As a result of the Data Breach notice, Plaintiff Denson spent time dealing with the consequences of the Data Breach, which includes time spent

verifying the legitimacy of the Notice of Data Breach and self-monitoring their accounts. This time has been lost forever and cannot be recaptured.

97. Additionally, Plaintiff Denson is very careful about sharing their sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

98. Plaintiff Denson stores any documents containing their sensitive PII in a safe and secure location or destroys the documents. Moreover, they diligently choose unique usernames and passwords for her various online accounts.

99. Plaintiff Denson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

100. Plaintiff Denson has a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

101. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

102. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII may have been accessed and/or acquired in the ransomware attack that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and Class Members on or around May 11, 2023 (the "Nationwide Class").

103. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

> All individuals who were employed by Defendants or one of the Dental Centers on or before February 22, 2023, and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and Class Members on or around May 11, 2023 (the "Employee Subclass").

104. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

> All individuals who were patients of Defendants or one of the Dental Centers on or before February 22, 2023, and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and Class Members on or around May 11, 2023 (the "Patient Subclass") (collectively, with the Nationwide Class, "the Classes").

105. Excluded from the Classes are the following individuals and/or entities:

Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

106. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

107. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. The total number of impacted individuals is expected to be significant as Defendants collected information about current and former employees and patients of more than 300 Dental Centers. Defendants reported to the Texas Attorney General that 1,262 individuals were impacted by the Data Breach and reported to the Massachusetts Attorney General that 426 individuals were impacted by the Data Breach.

108. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII of

Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual,

consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

109. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

110. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

111. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling

conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

112. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

113. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient

and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

114. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

115. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

116. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

117. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

118. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

119. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

120. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

121. Defendants knew or reasonably should have known that the failure to

exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

122. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendants' possession was adequately secured and protected.

123. Defendants also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII they were no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

124. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

125. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Nationwide Class. That special relationship arose because Defendants acquired

Plaintiff's and the Nationwide Class's confidential PII in the course of their business practices.

126. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

127. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

128. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

129. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendants.

130. Plaintiffs and the Nationwide Class had no ability to protect their PII

that was in, and possibly remains in, Defendants' possession.

131. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

132. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

133. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

134. Defendants have admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

135. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendants' possession or control.

136. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

137. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

138. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

139. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII they were no longer required to retain pursuant to regulations and which Defendants had no reasonable need to maintain in an Internet-accessible environment.

140. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

141. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

142. There is a close causal connection between Defendants' failure to

implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

143. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised

as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

144. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

145. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

146. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs Brito, Coffey, and Williams and the Employee Subclass)

147. Plaintiffs Brito, Coffey, and Williams and the Employee Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

148. In obtaining employment from Defendants or one of the Dental Centers, Plaintiffs Brito, Coffey, and Williams and the Employee Subclass provided and entrusted their PII to Defendants.

149. Defendants required Plaintiffs Brito, Coffey, and Williams and the Employee Subclass to provide and entrust their PII as condition of obtaining employment from Defendants or one of the Dental Centers.

150. As a condition of obtaining employment from Defendants or one of the Dental Centers, Plaintiffs Brito, Coffey, and Williams and the Employee Subclass provided and entrusted their PII. In so doing, Plaintiffs Brito, Coffey, and Williams and the Employee Subclass entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs Brito, Coffey, and Williams and the Employee Subclass if their PII had been compromised or stolen.

151. Plaintiffs Brito, Coffey, and Williams and the Employee Subclass fully performed their obligations under the implied contracts with Defendants.

152. Defendants breached the implied contracts they made with Plaintiffs Brito, Coffey, and Williams and the Employee Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and by failing to provide

timely and accurate notice to them that PII was compromised as a result of the data breach.

153. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs Brito, Coffey, and Williams and the Employee Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

154. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs Brito, Coffey, and Williams and the Employee Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs Brito, Coffey, and Denson and the Patient Subclass)

155. Plaintiffs Brito, Coffey, and Denson and the Patient Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

156. In obtaining services from Defendants or one of the Dental Centers, Plaintiffs Brito, Coffey, and Denson and the Patient Subclass provided and entrusted their PII to Defendants.

157. Defendants required Plaintiffs Brito, Coffey, and Denson and the Patient Subclass to provide and entrust their PII as a condition of obtaining services from Defendants or one of the Dental Centers.

158. As a condition of obtaining services from Defendants or one of the Dental Centers, Plaintiffs Brito, Coffey, and Denson and the Patient Subclass provided and entrusted their PII. In so doing, Plaintiffs Brito, Coffey, and Denson and the Patient Subclass entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs Brito, Coffey, and Denson and the Patient Subclass if their PII had been compromised or stolen.

159. Plaintiffs Brito, Coffey, and Denson and the Patient Subclass fully performed their obligations under the implied contracts with Defendants.

160. Defendants breached the implied contracts they made with Plaintiffs Brito, Coffey, and Denson and the Patient Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

161. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs Brito, Coffey, and Denson and the Patient Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

162. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs Brito, Coffey, and Denson and the Patient Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

163. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

164. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

165. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Nationwide Class's PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further

compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

166. Plaintiffs and the Nationwide Class's have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiff's and the Nationwide Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendants' failure to delete PII they had no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiff.

167. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII of Plaintiffs and the Nationwide Class;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiffs harm.

168. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

d. engage third party auditors, consistent with industry standards, to test their systems for weakness and upgrade any such weakness found;

e. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test their systems for security vulnerabilities, consistent with industry standards;

g. implement an education and training program for appropriate employees regarding cybersecurity.

169. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

170. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Employee Subclass, the Patient Subclass and appointing Plaintiffs and their Counsel to represent such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and

audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class

Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: August 28, 2023

Respectfully Submitted,

/s/ *Ryan D. Maxey*
Michael N. Hanna (P81462)
MORGAN & MORGAN, P.A.
Attorney for Plaintiffs
2000 Town Center
Suite 1900

Southfield, MI 48075
Tel: (313) 251-1399
mhanna@forthepeople.com

Patrick A. Barthle
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
pbarthle@ForThePeople.com

Ryan D. Maxey*
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
(813) 448-1125
ryan@maxeyfirm.com

Attorneys for Plaintiff Brito and the Proposed Class

Joseph M. Lyon*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Attorneys for Plaintiff Coffey and the Proposed Class

Andrew Shamis*
SHAMIS & GENTILE, P.A.
14 NE 1st Ave, Suite 705
Miami, FL 33132
Phone: (305) 479-2299
Fax: (786) 623-0915
ashamis@shamisgentile.com

Attorneys for Plaintiffs Williams and Denson and the Proposed Class

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that on August 28, 2023, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

/s/ Ryan D. Maxey

Ryan D. Maxey